

ABELIAN GROUPS, HOMOMORPHISMS AND CENTRAL AUTOMORPHISMS OF NILPOTENT GROUPS

AYAN MAHALANOBIS

1. INTRODUCTION

It is natural to try to find a necessary and sufficient condition for a finite group to have an abelian central automorphism group. In this paper we find a necessary and sufficient condition in case when the group is finite and nilpotent, see Theorem 4.1. Since a nilpotent group is the direct product of its Sylow subgroups, finding a necessary and sufficient condition for a nilpotent group is equivalent to finding a necessary and sufficient condition for a p -group. So from now on we work with p -groups. Also, we saw in [13, 14] that a p -group with a non-trivial abelian subgroup of its automorphism group can be used to build a key exchange protocol, useful in public key cryptography. This author in [13, 14] used a family of groups with commutative central automorphism group in a Diffie-Hellman type key exchange protocol.

The most notable of the recent publications in the direction of understanding the central automorphisms of a finite p -group are [3, 4, 8, 11, 2]. Jamali and Mousavi in [11] provide a necessary and sufficient condition for a p -group G of class 2, for an odd prime p , to have an elementary abelian central automorphism group and Curran [2] studies groups which have an abelian automorphism group, i.e., Miller groups. In a Miller group all automorphisms are central, so our work contributes to the study of the central automorphisms of nilpotent groups as well as the study of Miller groups. For an introduction to Miller groups see [6, 15] or [14, Section 2.7].

Definition (PN Group). *A group G is a purely non-abelian group if it doesn't have any nontrivial abelian direct factor.*

Adney and Yen in [1, Theorem 4] proved a necessary and sufficient condition for a finite PN p -group of class 2 to have an abelian central automorphism group. In this article we extend that result and to a certain extent their argument to arbitrary finite PN p -groups. We split the problem into three parts:

Ayan.Mahalanobis@stevens.edu.

- a Reduce the problem to a problem about abelian groups and homomorphisms between abelian groups.
- b Solve the problem in finite abelian groups.
- c Bring the solution from abelian groups back to non-abelian finite PN p -groups.

This is not the first time that the theory of abelian groups has been used in understanding the automorphisms of non-abelian p -groups. Sanders [16] used a technique quite similar to ours to count the number of central automorphisms in a finite PN (purely non-abelian) p -group.

2. CENTRAL AUTOMORPHISMS

Let $\text{Aut}_c(G)$ be the group of central automorphisms of a group G . An automorphism $\sigma \in \text{Aut}(G)$ is called a central automorphism if $g^{-1}\sigma(g) \in Z(G)$ for all $g \in G$, or equivalently, central automorphisms are the centralizer of the group of inner automorphisms.

There is another way to think about the central automorphisms. Let $\sigma \in \text{Aut}_c(G)$, then corresponding to $g \in G$ there is a $z_{g,\sigma} \in Z(G)$ such that $\sigma(g) = gz_{g,\sigma}$. Corresponding to $\sigma \in \text{Aut}_c(G)$ one can define a map $\phi_\sigma : G \rightarrow Z(G)$ as follows:

$$\phi_\sigma(g) = z_{g,\sigma}$$

It is straightforward to show that the map ϕ_σ is a homomorphism. Hence corresponding to $\sigma \in \text{Aut}_c(G)$ there is $\phi_\sigma \in \text{Hom}(G, Z(G))$. It is known that for PN groups the converse is true, see [1, Theorem 1].

There is a connection [1, Theorem 3] between commutativity of the group of central automorphisms $\text{Aut}_c(G)$ and commutativity of the homomorphisms ϕ_σ .

Assume that $\text{Aut}_c(G)$ is commutative, then for two maps $\tau, \sigma \in \text{Aut}_c(G)$ we have that $\tau(\sigma(g)) = \sigma(\tau(g))$ which is the same as

$$g\phi_\sigma(g)\phi_\tau(g)\phi_\sigma(\phi_\tau(g)) = g\phi_\tau(g)\phi_\sigma(g)\phi_\tau(\phi_\sigma(g))$$

implying, $\sigma, \tau \in \text{Aut}_c(G)$ commute if and only if $\phi_\sigma, \phi_\tau \in \text{Hom}(G, Z(G))$ commute. Notice that since $Z(G)$ is an abelian group hence $\phi_\sigma(G') = 1$. So corresponding to $\phi_\sigma : G \rightarrow Z(G)$ one can define $\phi'_\sigma : \frac{G}{G'} \rightarrow Z(G)$ as $\phi'_\sigma(xG') = \phi_\sigma(x)$. Clearly ϕ'_σ is a homomorphism.

Consider the map $\lambda : Z(G) \rightarrow G/G'$ given by the diagram

$$(1) \quad Z(G) \xrightarrow{\iota} G \xrightarrow{\pi} G/G'$$

where ι and π are the inclusion and the natural surjection respectively.

Theorem 2.1. *Let $\sigma, \tau \in \text{Aut}_c(G)$ then $\sigma \circ \tau = \tau \circ \sigma$ if and only if $\phi'_\sigma \circ \lambda \circ \phi'_\tau = \phi'_\tau \circ \lambda \circ \phi'_\sigma$.*

Proof. The proof follows from the above discussion. •

This theorem enables us to think about commutativity of the group of central automorphisms of a nonabelian group G in terms of abelian groups $\frac{G}{G'}$ and $Z(G)$ and homomorphisms between these abelian groups. So the problem “when is $\text{Aut}_c(G)$ commutative?” for a PN group is transformed into a problem involving abelian groups and homomorphisms between abelian groups.

This also enables us to ask more general questions about abelian groups and homomorphisms between abelian groups that is the object of our study in the next section.

3. C-MAPS

Definition (c-map). *Let A and B be abelian groups and $\lambda : A \rightarrow B$ a homomorphism. Then λ is a c-map if $f\lambda g = g\lambda f$ for all $f, g \in \text{Hom}(B, A)$. The set of all c-maps form a subgroup of $\text{Hom}(A, B)$. We call λ a trivial c-map if $f\lambda g = 0$ for all $f, g \in \text{Hom}(B, A)$.*

In this section we investigate necessary and sufficient conditions for two finite abelian groups A and B and $\lambda : A \rightarrow B$ a homomorphism between them to be a c-map. Of course if $\lambda \equiv 0$ then trivially $f\lambda g = 0$ for any $f, g \in \text{Hom}(B, A)$ and λ is a c-map.

For the rest of this section we fix A and B to be two finite nonzero abelian p -groups. From the fundamental theorem of finite abelian groups, we have

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_n \quad n \geq 1$$

$$B = B_1 \oplus B_2 \oplus \cdots \oplus B_m \quad m \geq 1$$

where

$$A_i = \langle a_i \rangle, \quad \exp(A_i) = p^{\alpha_i} \quad \text{and} \quad \alpha = \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$$

$$B_i = \langle b_i \rangle, \quad \exp(B_i) = p^{\beta_i} \quad \text{and} \quad \beta = \beta_1 \geq \beta_2 \geq \cdots \geq \beta_m$$

are decompositions of A and B as direct sums of cyclic p -groups. For the rest of this article we fix A_1, A_2, \dots, A_n as a fixed decomposition of A and B_1, B_2, \dots, B_m as a fixed decomposition of B and a_i a fixed generator for A_i , $1 \leq i \leq n$ and b_i a fixed generator for B_i , $1 \leq i \leq m$.

If $\lambda : A \rightarrow B$ is a homomorphism, we can write $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_m$ where $\lambda_i : A \rightarrow B_i$ is defined as follows:

$$\lambda_i(a) = \pi_i \lambda(a)$$

where $\pi_i : B \rightarrow B_i$ is the projection. We can abuse the notation a little bit and consider $\lambda_i : A \rightarrow B$. Of course, one can formalize this trivially. It is easy to see that if each λ_i is a c-map, then λ is a c-map.

Let $\mathcal{R} = \{x \in A \mid |x| \leq p^b\}$. It is known that

$$\mathcal{R} = \sum_{f \in \text{Hom}(B, A)} f(B)$$

and since \mathcal{R} is an abelian group contained in A and if $x_1 + x_2 + \dots + x_n \in \mathcal{R}$ then from the definition of \mathcal{R} it follows that $x_i \in \mathcal{R}$ for $i = 1, 2, \dots, n$. Hence $\mathcal{R} = \mathcal{R}_1 \oplus \mathcal{R}_2 \oplus \dots \oplus \mathcal{R}_n$ where $\mathcal{R}_i = \langle r_i \rangle$ and $\mathcal{R}_i = \mathcal{R} \cap A_i$ for each i . We assume that $\exp(\mathcal{R}_1) = p^{n_1}$ and $\exp(\mathcal{R}_2 \oplus \mathcal{R}_3 \oplus \dots \oplus \mathcal{R}_n) = p^{n_2}$. Clearly $a \geq n_1 \geq n_2$.

Let $e_{ij} : B \rightarrow A$ be defined as

$$(2) \quad e_{ij}(b_k) = \begin{cases} p^{\max(0, \alpha_i - \beta_j)} a_i & \text{if } j = k \\ 0 & \text{otherwise} \end{cases}$$

It follows from [17, Section 5.8] that $\{e_{ij}\}$, $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$ is a basis for $\text{Hom}(B, A)$ under addition.

From Equation 2 either $r_i = a_i$ or $r_i = p^{\alpha_i - \beta_1} a_i$. Since β_1 is the maximum possible hence $\alpha_i - \beta_1$ is the least possible for a fixed i and for all j ($1 \leq j \leq m$). From this we conclude that $e_{i1}(b_1) = r_i$ for all i .

We state some easy and well known facts in the following lemma whose proof follows from the above discussion.

Lemma 3.1. (i) $\mathcal{R} = A[p^b]$.

(ii) $\mathcal{R} = \mathcal{R}_1 \oplus \mathcal{R}_2 \oplus \dots \oplus \mathcal{R}_n$ where $\mathcal{R}_i = \mathcal{R} \cap A_i$.

(iii) If $\mathcal{R}_i = \langle r_i \rangle$, then $r_i = a_i$ if $b \geq \alpha_i$ or $r_i = p^{\alpha_i - \beta_1} a_i$ if $b < \alpha_i$.

(iv) $e_{i1}(b_1) = r_i$ for all i .

(v) $e_{1j}(b_j) = p^{\max(0, n_1 - \beta_j)} r_1$ for $j > 1$.

Theorem 3.2. A homomorphism $\lambda : A \rightarrow B$ is a c -map if and only if $e_{ij}\lambda e_{kl} = 0$ whenever $i \neq k$ or $j \neq l$.

Proof. Let $f\lambda g = g\lambda f$ for all $f, g \in \text{Hom}(B, A)$ then $e_{ij}\lambda e_{kl} = e_{kl}\lambda e_{ij}$. If $i \neq k$ then $e_{ij}\lambda e_{kl} = 0$. Since the image of $e_{ij}\lambda e_{kl}$ is in $A_i \cap A_k$ where $A_i \cap A_k = 0$ whenever $i \neq k$. If $j \neq l$ then $e_{kl}\lambda e_{ij}(b_l) = 0$. Hence, $e_{ij}\lambda e_{kl} = 0$ whenever $i \neq k$ or $j \neq l$.

Conversely, notice that any $f \in \text{Hom}(B, A)$ can be written as $f = \sum_{j=1}^m \sum_{i=1}^n n_{ij} e_{ij}$ where $n_{ij} \in \mathbb{Z}$. Hence we can write $f = \sum_{j=1}^m \sum_{i=1}^n n_{ij} e_{ij}$ where

$n_{ij} \in \mathbb{Z}$ and $g = \sum_{j=1}^m \sum_{i=1}^n n'_{ij} e_{ij}$ where $n'_{ij} \in \mathbb{Z}$. Hence

$$\begin{aligned}
& f\lambda g \\
&= \left(\sum_{j=1}^m \sum_{i=1}^n n_{ij} e_{ij} \right) \lambda \left(\sum_{k=1}^m \sum_{l=1}^n n'_{kl} e_{kl} \right) \\
&= \sum_{j=1}^m \sum_{i=1}^n (n_{ij} e_{ij} \lambda n'_{ij} e_{ij}) \quad \text{since } e_{ij} \lambda e_{kl} = 0 \text{ whenever } i \neq k \text{ or } j \neq l \\
&= \sum_{j=1}^m \sum_{i=1}^n n_{ij} n'_{ij} (e_{ij} \lambda e_{ij}) \\
&= \sum_{j=1}^m \sum_{i=1}^n n'_{ij} n_{ij} (e_{ij} \lambda e_{ij}) = g\lambda f.
\end{aligned}$$

•

We use the above theorem to prove:

Theorem 3.3. *A homomorphism $\lambda : A \rightarrow B$ is a c-map if and only if*

- (3) $\lambda(r_u) \in p^{n_1} B \quad u > 1$
- (4) $\lambda_1(r_1) \in \langle p^{k'} b_1 \rangle \quad k' = \min(n_1, \max(n_2, \beta_2))$
- (5) $\lambda_j(r_1) \in \langle p^{n_1} b_j \rangle \quad j > 1.$

Moreover, if λ satisfies the above conditions and $\langle \lambda_1(r_1) \rangle = \langle p^k b_1 \rangle$ where $k' \leq k < n_1$, then $\lambda(\mathcal{R}) = p^k B_1$.

Proof. We assume that conditions (3), (4) and (5) are satisfied. If $u > 1$ then $\lambda(r_u) \in p^{n_1} B$. Hence $e_{st} \lambda e_{uv} = 0$ for all s, t and v . If $u = 1$ then for $s > 1$, $e_{st} \lambda e_{uv}(b_v) \in \mathcal{R}_s$. Now since $\exp(\mathcal{R}_s) \leq p^{n_2}$ and $\lambda_j(r_1) \in \langle p^{n_2} b_j \rangle$ for $1 \leq j \leq m$, hence we have $e_{st} \lambda e_{uv} = 0$. From the earlier discussion it follows that $e_{11}(b_1) = r_1$. Now notice that for $t > 1$, $e_{1t} \lambda e_{11}(b_1) = e_{1t} \lambda(r_1) = 0$ and $e_{11} \lambda e_{1t}(b_t) = e_{11} \lambda(p^{\max(0, n_1 - \beta_t)} r_1) = 0$, from the definition of k' .

Conversely, we assume that $e_{st} \lambda e_{uv} = 0$ whenever $s \neq u$ or $t \neq v$. Now $e_{11}(b_1) = r_1$ then for a $j > 1$ $e_{1j} \lambda e_{11} = 0$. That says that

$$e_{1j} \lambda_j(r_1) = 0 \text{ for each } j > 1$$

Now from Equation 2 either $e_{1j}(b_j) = r_1$ or $e_{1j}(b_j) = p^{n_1 - \beta_j} r_1$. In the first case clearly $\lambda_j(r_1) \in \langle p^{n_1} b_j \rangle$. In the second case it follows from $e_{1j} \lambda(r_1) = 0$ that $\lambda_j(r_1) = p^{\beta_j} b_j = 0$. In either case $\lambda_j(r_1) \in \langle p^{n_1} b_j \rangle$. This proves (5).

Pick a $u > 1$, then $e_{1j} \lambda e_{u1} = 0$ for all j . This implies that $e_{1j} \lambda(r_u) = 0$ for all j . Since $e_{1j}(b_j) = r_1$ or $p^{n_1 - \beta_j} r_1$ hence $\lambda_j(r_u) \in \langle p^{n_1} b_j \rangle$ or $\lambda_j(r_u) = 0$ for $u > 1$ and all j . This proves (3).

Choose $u > 1$ such that $\exp(\mathcal{R}_2 \oplus \mathcal{R}_3 \oplus \cdots \oplus \mathcal{R}_n) = \exp(\mathcal{R}_u) = p^{n_2}$ and then we have that $e_{u1}(b_1) = r_u$, then clearly $e_{u1}\lambda e_{11} = 0$ implies that $e_{u1}\lambda(r_1) = 0$, hence $\lambda_1(r_1) \in \langle p^{n_2}b_1 \rangle$.

On the other hand $e_{11}\lambda e_{1j} = 0$ for $j > 1$ implies that $e_{11}\lambda(p^{\max(0, n_1 - \beta_j)}r_1) = 0$ which implies that $p^{\max(0, n_1 - \beta_j)}e_{11}\lambda(r_1) = 0$ for all $j > 1$. This gives us that $\lambda_1(r_1) \in \langle p^{k'}b_1 \rangle$. The above two arguments proves (4).

The later assertion of the theorem clearly follows from the fact that $\beta_2 \leq k$ and hence $p^{n_1}b_j = 0$ for all $j > 1$. •

Corollary 3.4. *If $n_1 = n_2$ and $\lambda : A \rightarrow B$ is a c-map then λ is a trivial c-map.*

Proof. It follows from Theorem 3.3, since $k' = n_1$ that $\lambda(r_i) \in p^{n_1}B$ for all i , hence $f\lambda(r_i) = 0$ for all i and hence $f\lambda g = 0$. •

Corollary 3.5. *If $b = n_1$ and λ is a c-map, then $\lambda(\mathcal{R}_2 \oplus \mathcal{R}_3 \oplus \cdots \oplus \mathcal{R}_n) = 0$. This automatically implies that $\lambda(\mathcal{R})$ is cyclic.*

Proof. From Theorem 3.3 it follows that $\lambda(r_i) = 0$ for $i > 1$. •

Now assume there is a j such that $\exp(B_j) = \exp(B_1)$ and $j > 1$. Then clearly $e_{1j}(b_j) = r_1$. If λ is a c-map then $e_{11}\lambda e_{1j}(b_j) = 0$ implying that $e_{11}\lambda(r_1) = 0$. This tells us that $\lambda_1(r_1) = p^{n_1}b_1$ which makes λ a trivial c-map. We just established that a necessary condition for λ to be a nontrivial c-map is that $\exp(B_1) > \exp(B_j)$ for $j > 1$.

If $\lambda : A \rightarrow B$ is any homomorphism, let $p^c = \exp(\ker(\lambda))$, clearly $c \leq a$. We now find a necessary and sufficient condition for $\ker(\lambda) \subseteq \mathcal{R}$. Recall that $\mathcal{R} = A[p^b]$.

Lemma 3.6. *$\ker(\lambda) \subseteq \mathcal{R}$ if and only if $c \leq n_1$.*

Proof. Let $\ker(\lambda) \subseteq \mathcal{R}$. Since $p^{n_1}\mathcal{R} = 0$ hence $p^{n_1}\ker(\lambda) = 0$. This proves that $c \leq n_1$. Conversely, assume that $c \leq n_1$. Let $x \in \ker(\lambda)$ then $p^{n_1}x = 0$ hence $x \in \mathcal{R}$. •

The next lemma comes in handy to settle the question: if $c \geq n_1$ then are there any nontrivial c-maps?

Lemma 3.7. $p^c B = \bigcap_{f: B \rightarrow \ker(\lambda)} \ker(f)$.

Proof. Let $x \in p^c B$ then $x = p^c y$ for some $y \in B$. Then for any $f \in \text{Hom}(B, \ker(\lambda))$, $f(x) = p^c f(y) = 0$, since the exponent of $\ker(\lambda)$ is c . So $p^c B \subseteq \bigcap_{f: B \rightarrow \ker(\lambda)} \ker(f)$. Conversely, assume that $x \notin p^c B$ then the image

of x in $\frac{B}{p^c B}$ is nontrivial and $\exp\left(\frac{B}{p^c B}\right) = p^c = \exp(\ker(\lambda))$. Hence there is a $f \in \text{Hom}(B, \ker(\lambda))$ such that $f(x) \neq 0$. •

Taking the two previous lemmas together we show that

Lemma 3.8. *If $\lambda : A \rightarrow B$ is a c -map then $\lambda(\mathcal{R}) \subseteq p^c B$. It follows that if λ is a c -map and $c \geq n_1$ then λ is a trivial c -map.*

Proof. Since λ is a c -map, hence $F\lambda g = g\lambda F$ where $F \in \text{Hom}(B, \ker(\lambda))$ and $g \in \text{Hom}(B, A)$. Then clearly $F\lambda g = 0$ for all $g \in \text{Hom}(B, A)$. Hence $F\lambda(\mathcal{R}) = 0$ for all $F \in \text{Hom}(B, \ker(\lambda))$. Hence

$$\lambda(\mathcal{R}) \subseteq \bigcap_{F: B \rightarrow \ker(\lambda)} \ker(F) = p^c B.$$

The rest of the argument follows from the fact that $\exp(\mathcal{R}) = p^{n_1}$. •

We just saw that for all intended purposes of understanding c -maps $c \geq n_1$ is irrelevant, because then λ is a trivial c -map. So, from now on we will work with $c < n_1$ which implies that $\ker(\lambda) \subseteq \mathcal{R}$.

This has little relevance to the flow of arguments towards the proof of the main result but is of independent interest. Using the same method as above one can easily prove that

$$p^a B = \bigcap_{f: B \rightarrow A} \ker f.$$

This yields a lemma, whose proof we leave to the reader and is corroborated by Theorem 3.3:

Lemma 3.9. *A homomorphism λ is a trivial c -map if and only if $\lambda(\mathcal{R}) \subseteq p^{n_1} B$.*

We are now in a position to prove the main theorem of this article.

Theorem 3.10. *Let $\lambda : A \rightarrow B$ be a homomorphism. Then λ is a non-trivial c -map if and only if*

$$\begin{aligned} \lambda(\mathcal{R}) &= p^k B \quad \text{where } c \leq k < n_1 \\ \text{and } \frac{\mathcal{R}}{\ker(\lambda)} &\text{ is cyclic.} \end{aligned}$$

Proof. The only if part follows from Theorem 3.3 and Lemma 3.8.

To see the if part, assume that $\lambda(\mathcal{R}) = p^k B$ where $c \leq k < n_1$ and $\frac{\mathcal{R}}{\ker(\lambda)}$ is cyclic. Without loss of generality we assume that $\frac{\mathcal{R}}{\ker(\lambda)} \cong \langle p^k b_1 \rangle$. Hence there is some $r \in \mathcal{R}$ such that $\lambda(r) = p^k b_1$. Also from $n_1 > c$, it follows that $|r| = n_1$. We show that $f\lambda g(b_i) = 0$ for all $f, g \in \text{Hom}(B, A)$ and $i \geq 2$.

It is clear that $|b_i| \leq p^k$ for $i \geq 2$ and $g(b_i) = sr + u$ where $u \in \text{Ker}\lambda$ and $p^{n_1-k}|s$. Then $s = s'p^{n_1-k}$. Hence $f(\lambda(s'p^{n_1-k}r + u)) = f(s'p^{n_1}b_1) = 0$ and this proves the theorem. \bullet

It is interesting to note what happens in case of a c-map λ such that $\exp(\ker(\lambda)) = \exp(\text{coker}(\lambda))$ which implies that $c \leq b$.

Notice that $p^{b-c}p^cB = p^bB = 0$. Now if $\lambda(x) \in p^cB$ then $\lambda(p^{b-c}x) = 0$, i.e., $p^{b-c}x \in \ker(\lambda)$. This says that $p^cp^{b-c}x = p^bx = 0$ which implies $x \in \mathcal{R}$. Now assume that $\exp(\ker(\lambda)) = \exp(\text{coker}(\lambda))$ then we have that $p^cB \subseteq \text{Image}(\lambda)$. Hence for any $y \in p^cB$ there is a $x \in A$ such that $\lambda(x) = y$. This implies that $x \in \mathcal{R}$. Hence $p^cB \subseteq \lambda(\mathcal{R})$. Using Lemma 3.8 we just proved the following lemma:

Lemma 3.11. *Let $\lambda : A \rightarrow B$ be a c-map and $\exp(\ker(\lambda)) = \exp(\text{coker}(\lambda))$ then $\lambda(\mathcal{R}) = p^cB$.*

4. BACK TO p -GROUPS

In this section we use the theorems from the last section to find a necessary and sufficient condition, in the same spirit as in Adney and Yen [1, Theorem 4], for the group of central automorphisms of a finite PN p -group G to be abelian. We have seen before that there is a one-to-one correspondence between the central automorphisms in G and homomorphisms from $\frac{G}{G'}$ to $Z(G)$. Now the central automorphisms commute if and only if $\lambda : Z(G) \rightarrow \frac{G}{G'}$ defined by $\lambda(x) = xG'$ is a c-map. We use all the notation from the last section with the understanding that $Z(G)$ represents A and $\frac{G}{G'}$ represents B . Since the group G is no longer abelian, even though $\frac{G}{G'}$ and $Z(G)$ are abelian, we will no longer use $+$ to denote the group operation. Clearly then the kernel of λ is $Z(G) \cap G'$. Notice that for a p -group G of class 2, $G' \subseteq Z(G)$ and $\exp(G') = \exp\left(\frac{G}{Z(G)}\right)$. This means that $\exp(G') \leq \exp\left(\frac{G}{G'}\right)$. This clearly implies that $c \leq b$.

Theorem 4.1. *Let G be a PN p -group and $p^c = \exp(Z(G) \cap G')$. Then the central automorphisms of G commute if and only if either*

$$\lambda(\mathcal{R}) \subseteq \left(\frac{G}{G'}\right)^{p^{n_1}}$$

or

$$\lambda(\mathcal{R}) = \left(\frac{G}{G'}\right)^{p^k} \quad \text{where } c \leq k < n_1$$

and $\frac{\mathcal{R}}{Z(G) \cap G'}$ is cyclic.

Proof. This theorem follows from Theorem 3.10. Notice that λ in this case is the map from Equation 1. •

We should mention the relation of our theorem with that of the [1, Theorem 4]. There the authors work only with p -groups of class 2. In that case we have that $\ker(\lambda) = \text{coker}(\lambda)$ and hence $\lambda(\mathcal{R}) = p^c B$ which is the same as Adney and Yen's condition $\mathcal{R} = \mathcal{K}$. Again since in a p -group of class 2, $\ker(\lambda) = G'$ their condition reads like $\frac{\mathcal{R}}{G'} = \langle x_1^{p^c} G' \rangle$.

Acknowledgement: The author wishes to thank Fred Richman for his help and guidance in preparation of this manuscript. The author is indebted to the referee for his comments and suggestions which has helped in a better presentation of this article.

REFERENCES

- [1] A. Adney and T. Yen. Automorphisms of a p -group. *Illinois Journal of Mathematics*, 9:137–143, 1965.
- [2] M. Curran. Semidirect product groups with abelian automorphism groups. *Journal of the Australian Mathematical Society*, Series A(42):84–91, 1987.
- [3] M. Curran. Finite groups with central automorphism group of minimal order. *Mathematical Proceedings of the Royal Irish Academy*, 104A(2):223–229, 2004.
- [4] M. Curran and D. McCaughan. Central automorphisms of finite groups. *Bulletin of the Australian Mathematical Society*, 34:191–198, 1986.
- [5] M. Curran and D. McCaughan. Central automorphisms that are almost inner. *Communications in Algebra*, 29(5):2081–2087, 2001.
- [6] B. E. Earnley. *On finite Groups whose group of automorphisms is abelian*. PhD thesis, Wayne State University, 1975.
- [7] T. Fournelle. Elementary abelian p -groups as automorphism group of infinite group. *I. Math. Z.*, 167:259–270, 1979.
- [8] T. A. Fournelle. Automorphisms of nilpotent groups of class two with small rank. *Journal of the Australian Mathematical Society. Series A*, 39:121–131, 1985.
- [9] L. Fuchs. *Infinite Abelian Groups*, volume 1. Academic Press, 1970.
- [10] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002. (<http://www.gap-system.org>).

- [11] A.-R. Jamali and H. Mousavi. On the central automorphism group of finite p -groups. *Algebra Colloquium*, 9(1):7–14, 2002.
- [12] I. Kaplansky. *Infinite Abelian Groups*. The University of Michigan Press, 1969.
- [13] A. Mahalanobis. Diffie-Hellman key exchange protocol and non-abelian nilpotent groups. Technical report, <http://eprint.iacr.org/2005/110>, 2005.
- [14] A. Mahalanobis. *Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups*. PhD thesis, Florida Atlantic University, August 2005. <http://eprint.iacr.org/2005/223>.
- [15] M. Morigi. On p -groups with abelian automorphism group. *The Mathematical Journal of the University of Padova*, 92:47–58, 1994.
- [16] P. R. Sanders. The central automorphism of a finite group. *Journal of the London Mathematical Society*, 44:225–228, 1969.
- [17] W. Scott. *Group Theory*. Dover, 1964.

DEPARTMENT OF MATHEMATICAL SCIENCES, STEVENS INSTITUTE OF TECHNOLOGY,
HOBOKEN, NJ 07030, USA.